Open Journal of
Mathematical Sciences

PSR Press

Article

A closer look at multiplication table of finite rings

Muhammad Tufail[1],* and Rabiha Qazi [1]

[1] Department of Mathematics, COMSATS University Islamabad, Attock, 43600 Pakistan.; rabbiyaqazi02@gmail.com

* Correspondence: tufail.rings@gmail.com

Received: 11 June 2018; Accepted: 4 September 2019; Published: 21 September 2019.

Abstract: The article investigates the behaviour of the multiplication table of the ring $\mathbb{Z}_n$. To count the number of 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$, conclusively an explicit formula is induced for any $n \geq 2$.

Keywords: Finite rings, modular arithmetic, multiplication table, congruences, Chinese remainder theorem.

MSC: 05C25.

1. Introduction

In finite algebra, $\mathbb{Z}_n$ is playing a dominant role. They are gears for studying the integers. Congruences modulo n is a fundamental relation in the integers and any statement concerning modulo n is equivalent to a statement about $\mathbb{Z}_n$. Although it is easier or it provides better insight, to study a statement about the congruences in the integers in terms of $\mathbb{Z}_n$. In general algebraic theories, $\mathbb{Z}_n$ are the fundamental building piles. All finite fields are constructed using $\mathbb{Z}_p$ for some prime p. The algebraic systems $\mathbb{Z}_n$, were initially studied in the nineteenth century without any view towards practical applications, simply because they had a natural and necessary role to play the development of the algebra, they are now absolutely fundamental in modern digital engineering, algorithms for digital communications, for error detection and correction, for cryptography, and for digital signal processing, all employ $\mathbb{Z}_n$. The set $\mathbb{Z}_n$ of integers modulo n forms a ring under addition and multiplication. For multiplication, the set of congruence classes modulo n that are coprime to n satisfy the axioms for an abelian group. Indeed, its quite captivating to deal with $\mathbb{Z}_n$.

In this paper, we discuss an interesting property about the multiplication table of $\mathbb{Z}_n$ that is "how many 1s appears on the main diagonal of the multiplication table of $\mathbb{Z}_n$?". By constructing some multiplication table of $\mathbb{Z}_n$ for the distinct values of n, and counting the number of 1s on the main diagonal, we observe it carefully because we find it very interesting. Finally, an explicit formula is generalized to count the number of 1s on the diagonals of the multiplication table of $\mathbb{Z}_n$, for any n. Starting with a Lemma which states that the number of solutions of the equation $X^2 = 1$ in a ring R is equal to the number of 1s appear on the main diagonal of the multiplication table of R (Lemma 2.1). This idea comes after reviewing an article entitled, " what is special about the divisors of 24" [1]. The main theorem of this article stated that " In the multiplication table of the ring $\mathbb{Z}_n$, the $1s$ appears only on the diagonal (never off diagonal) if and only if n is a divisor of 24". Similar diagonal property was also studied later in [2]. These studies appeals us to think more about the multiplication table of $\mathbb{Z}_n$.

We draw many multiplication tables of $\mathbb{Z}_n$ for different values of n to investigate some hidden properties. Let's have a look on the multiplication table of $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$ and $\mathbb{Z}_8$.

Table 1. Multiplication table of $\mathbb{Z}_4$

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note that, multiplication Table 1 for $\mathbb{Z}_4$ has two $1s$ on diagonal, $\mathbb{Z}_5$ has two $1s$ on diagonal (Table 2), similarly $\mathbb{Z}_6$, $\mathbb{Z}_7$ has two $1s$ on diagonal (Tables 3 and 4) but $\mathbb{Z}_8$ has four 1s on diagonal (Table 5). It appear

Table 2. Multiplication table of $\mathbb{Z}_5$

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 3. Multiplication table of $\mathbb{Z}_6$

•	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 4. Multiplication table of $\mathbb{Z}_7$

•	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 5. Multiplication table of $\mathbb{Z}_8$

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

interesting to me to find an (explicit formula) algorithm to count the number of 1*s* on the main diagonal of multiplication table of $\mathbb{Z}_n$ for any n so that one can count the 1*s* on the main diagonal without actually drawing the multiplication table. Initiating with a Lemma.

Throughout this paper all the rings are commutative with unity. Any unexplained material is standard as in [3].

2. Main results

Lemma 1. *The number of solutions of the equation $X^2 = 1$ in a finite ring R is equal to the number of* 1*s appears on the main diagonal of multiplication table of R.*

Table 6. Multiplication table of R

$\bullet$	-	a	-
a	-	1	-
-	-	-	-

Proof. Let $a \in R$ be the solution of $X^2 = 1$. Then $a^2 = 1$. So the entry corresponding to (a, a), which is on main diagonal, will be 1.

Conversely, if 1 appears on main diagonal then the entries opposite to 1 will be same element say $a \in R$. That's mean $a \cdot a = 1$ and we have a, a solution of $X^2 = 1$ in R (see Table 6). □

Remark 1. In order to count the the number of 1s on main diagonal, it is enough to count the solution of the equation $X^2 = 1$ in $\mathbb{Z}_n$.

Theorem 2. *Let R and S be rings. If $X^2 = 1$ has m solutions in R and n solutions in S, then $X^2 = 1$ has mn solution in the ring $R \oplus S$.*

Proof. If $a \in R$ and $b \in S$ be the solutions of $X^2 = 1$, then (a, b) is a solution of $X^2 = 1$ in $R \oplus S$. Therefore, if S_1 is the solution set of $X^2 = 1$ in R and S_2 is the solution set of $X^2 = 1$ in S, then $S_1 \times S_2$ is the solution set of $X^2 = 1$ in $R \oplus S$.
Hence, $|S_1 \times S_2| = |S_1| \times |S_2| = m \times n = mn$. □

Theorem 3. *Exactly two 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_p$ for any prime p.*

Proof. By using Lemma 1, in order to count the number of 1*s* on the main diagonal it is enough to count the solutions of the equation $X^2 = 1$ in $\mathbb{Z}_p$. Let $\bar{a} \in \mathbb{Z}_p$ be the solution of $X^2 = 1$.
$\Rightarrow \bar{a}^2 = \bar{1} \Rightarrow \bar{a}^2 - \bar{1} = \bar{0} \Rightarrow p|a^2 - 1 = (a-1)(a+1) \Rightarrow p|a-1$ or $p|a+1$
$\Rightarrow \overline{a-1} = \bar{0}$ or $\overline{a+1} = \bar{0} \Rightarrow \bar{a} - \bar{1} = \bar{0}$ or $\bar{a} + \bar{1} = \bar{0} \Rightarrow \bar{a} = \bar{1}$ or $\bar{a} = -\bar{1}$ in $\mathbb{Z}_p$. □

Theorem 4. *Exactly two 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_{p^2}$, where p is odd prime.*

Proof. By using Lemma 1, in order to count the number of 1*s* on the main diagonal it is enough to count the solution of the equation $X^2 = 1$ in $\mathbb{Z}_{p^2}$. Let $\bar{a} \in \mathbb{Z}_{p^2}$ be the solution of $X^2 = 1$. $\Rightarrow \bar{a}^2 = \bar{1} \Rightarrow \bar{a}^2 - \bar{1} = \bar{0}$ $\Rightarrow a^2 - 1 \equiv 0 \ (mod\ p^2) \Rightarrow p^2 \mid a^2 - 1 = (a-1)(a+1)$. Since an odd prime cannot divide $a-1$ and $a+1$ simultaneously, therefore, either (i) $p^2 \mid a-1$ and $p^2 \nmid a+1$ or (ii) $p^2|a+1$ and $p^2 \nmid a-1$. In the first case we obtain $\bar{a} - \bar{1} = \bar{0} \Rightarrow \bar{a} = \bar{1}$ in $\mathbb{Z}_{p^2}$ and in second case we obtain $\bar{a} = -\bar{1} = \overline{n-1}$ in $\mathbb{Z}_{p^2}$. □

Theorem 5. *Exactly two 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_{p^k}$ for any odd prime p and positive integer k.*

Proof. By using Lemma 1, in order to count the number of 1*s* on the main diagonal it is enough to count the solution of the equation $X^2 = 1$ in $\mathbb{Z}_{p^2}$. Let $\bar{a} \in \mathbb{Z}_{p^k}$ be the solution of $X^2 = 1$. $\Rightarrow \bar{a}^2 = \bar{1} \Rightarrow \bar{a}^2 - \bar{1} = \bar{0}$ $\Rightarrow a^2 - 1 \equiv 0 \ (mod\ p^k) \Rightarrow p^k \mid a^2 - 1 = (a-1)(a+1)$. Since an odd prime cannot divide $a-1$ and $a+1$ simultaneously, therefore, either (i) $p^k \mid a-1$ and $p^k \nmid a+1$ or (ii) $p^k|a+1$ and $p^k \nmid a-1$. In the first case we obtain $\bar{a} - \bar{1} = \bar{0} \Rightarrow \bar{a} = \bar{1}$ in $\mathbb{Z}_{p^k}$ and in second case we obtain $\bar{a} = -\bar{1} = \overline{n-1}$ in $\mathbb{Z}_{p^k}$. □

Theorem 6. *Exactly four 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_{2^k}$ where $k \geq 3$.*

Proof. By using Lemma 1, in order to count the number of 1*s* on the main diagonal, it is enough to count the solution of the equation $X^2 = 1$ in $\mathbb{Z}_{2^k}$. The congruence $x^2 \equiv 1 \ (mod\ 2^k)$, where k is an integer, $k \geq 3$, has exactly four incongruent solutions, cf. [4, Exercise 9.1, Problem 18, Page 301]. □

Theorem 7. *Let $n = 2^k p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_m^{\alpha_m}$, where $0 \leq k \leq 1$, p_is are distinct odd primes and α_is $\in \mathbb{Z}^+$ for all $i; 1 \leq i \leq m$. Then exactly 2^m number of 1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$.*

Proof. By Chinese Remainder Theorem, $\mathbb{Z}_n \cong \mathbb{Z}_{2^k} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. Therefore the number of $1s$ on the main diagonal of the multiplication table of $\mathbb{Z}_n$ is equal to the number of $1s$ on the main diagonal of multiplication table of $\mathbb{Z}_{2^k} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. Note that $x^2 \equiv 1 \pmod 2$ has exactly one solution. Hence by applying Theorems 2 and 5 we get that

$$\underbrace{2 \times 2 \times \cdots \times 2}_{m-times} = 2^m$$

$1s$ appear on the main diagonal of multiplication table of $\mathbb{Z}_n$. □

Theorem 8. *Let $n = 4 \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where $p_1,\ p_2,\ \dots,\ p_m$ are distinct odd primes and $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_m$ are positive integers. Then exactly 2^{m+1} $1s$ appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$.*

Proof. Using Chinese Remainder Theorem, $\mathbb{Z}_n \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. So the number of $1s$ on the main diagonal of the multiplication table of $\mathbb{Z}_n$ is equal to the number of 1s appear on the main diagonal of $\mathbb{Z}_4 \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. By applying Theorems 2 and 6, we get that

$$2 \times (\underbrace{2 \times 2 \times \cdots \times 2}_{m-times}) = 2^{m+1}$$

1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$. □

Theorem 9. *Let $n = 2^k \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where $k \geq 3$ and $p_1,\ p_2,\ \dots,\ p_m$ are distinct odd primes and $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_m$ are positive integers. Then exactly 2^{m+2} $1s$ appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$.*

Proof. Using Chinese Remainder Theorem, $\mathbb{Z}_n \cong \mathbb{Z}_{2^k} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. So the number of $1s$ on the main diagonal of the multiplication table of $\mathbb{Z}_n$ is equal to the number of 1s appear on the main diagonal of $\mathbb{Z}_{2^k} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}$. By applying Theorems 2 and 5, and 6 we get that

$$4 \times (\underbrace{2 \times 2 \times \cdots \times 2}_{m-times}) = 2^{m+2}$$

1s appear on the main diagonal of the multiplication table of $\mathbb{Z}_n$. □

Remark 2. It is important to mention here that one can continue to extend above results for many other classes of finite commutative rings.

Acknowledgments: The concept integrated with the substantial guidance of Dr. Shafiq ur Rehman, Assistant Professor in CUI Attock Campus. We are indebted to him, for his firm knowledge towards the field.

Author Contributions: All authors contributed equally to the writing of this paper. All authors read and approved the final manuscript.

Conflicts of Interest: "The authors declare no conflict of interest."

Bibliography

[1] Chebolu, S. K. (2012). What is special about the divisors of 24. *Mathematics Magazine, 85*(5), 366-372.

[2] Chebolu, S. K. & Mayers, M. (2013). What is special about the divisors of 12. *Mathematics Magazine, 86*(2), 143-146.

[3] Dummit, D. S., & Foote, R. M. *Abstract Algebra*, 3rd edition. Jhon Wiley and sons, 2004, USA.

[4] Rosen, K. H. *Elementry Number Theory and its Application.* Addison-Wesley Publishing company, 1984, USA.